



TRIBUNAL REGIONAL ELEITORAL DE GOIÁS
PRAÇA CÍVICA, 300 - Bairro CENTRO - CEP 74003-010 - Goiânia - GO - www.tre-go.jus.br

PORTARIA DG Nº 211, DE 16 DE JULHO DE 2025.

Institui a Norma de Gestão de Identidade e o Controle de Acesso Físico e Lógico ao ambiente cibernético do Tribunal Regional Eleitoral de Goiás.

O DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL DE GOIÁS, no uso da atribuição prevista no art. 46, inciso XVI, da Resolução TRE-GO nº 275, de 18 de dezembro de 2017 (Regulamento Interno), e considerando a instrução do procedimento SEI nº 23.0.000003970-5,

RESOLVE:

Art. 1º Fica instituída a Norma de Gestão de Identidade e Controle de Acesso Físico e Lógico relativa à segurança da informação e comunicação, a qual passa a integrar a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE n.º 23.644/2021.

CAPÍTULO I DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para efeitos desta norma, aplicam-se os termos e definições previstos no art. 2º da Portaria TSE n.º 444, de 08 de julho de 2021, aplicando-se, de forma subsidiária, aqueles estabelecidos no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, regulamentado por meio da Portaria GSI/PR n.º 93, de 18 de outubro de 2021.

CAPÍTULO II DOS PRINCÍPIOS

Art. 3º O controle de acesso é regido pelos seguintes princípios:

I - Necessidade de saber: os(as) usuários(as) deverão ter acesso somente às informações necessárias ao desempenho de suas tarefas;

II - Necessidade de uso: os(as) usuários(as) deverão ter acesso apenas aos ativos (equipamentos de TI, sistemas, aplicações, procedimentos, salas) necessários ao desempenho de suas tarefas;

III - Privilégio mínimo: deverão ser conferidos apenas os privilégios necessários para que o(a) usuário(a) realize a sua função na organização; e

IV - Segregação de funções: as funções desempenhadas no controle de acesso se dividem em pedido de acesso, autorização de acesso e administração de acesso.

CAPÍTULO III DO ESCOPO E DO ÂMBITO DE APLICAÇÃO

Art. 4º São objetivos desta norma:

I - estabelecer diretrizes para implantação de controles de acesso físico e lógico; e

II - assegurar a confidencialidade, integridade e disponibilidade dos ativos de informação e comunicação sob a responsabilidade deste Tribunal.

Art. 5º Este normativo se aplica a todos(as) os(as) magistrados(as), servidores(as) em exercício na Justiça Eleitoral de Goiás, servidores(as) efetivos(as) deste Regional em exercício em outro órgão público, inativos, estagiários(as), prestadores(as) de serviço, colaboradores(as) e usuários(as) externos(as), outros órgãos públicos ou entidades privadas contratadas ou com parcerias celebradas, acordos de cooperação de qualquer tipo, convênios e termos congêneres, que fazem uso dos ativos de informação e de processamento desta Especializada.

§ 1º Os contratos celebrados pelo Tribunal deverão atender aos requisitos desta portaria, bem como as normas referentes à proteção de dados pessoais.

§ 2º Os(As) usuários(as) relacionados no *caput* são corresponsáveis pela segurança da informação e comunicação, de acordo com os preceitos estabelecidos neste normativo.

§ 3º Os(As) usuários(as) de ativos de TI são responsáveis por:

- a) manter o ambiente seguro, incluindo criação de senhas seguras, conforme os padrões estabelecidos nesta norma;
- b) manter a confidencialidade das informações acessadas;
- c) informar imediatamente qualquer risco identificado ou presumido à segurança da instituição.

CAPÍTULO IV DO CONTROLE DE ACESSO LÓGICO

Seção I Do Gerenciamento de Acesso Lógico

Art. 6º O acesso aos sistemas de informação será assegurado, unicamente, ao(à) usuário(a) devidamente identificado(a) e autorizado(a).

§ 1º As credenciais de acesso são pessoais e intransferíveis, sendo vedado o compartilhamento de credenciais em qualquer situação, inclusive nas hipóteses de substituição temporária de função.

§ 2º Todas as ações e atividades executadas pelo(a) usuário(a), utilizando suas credenciais de acesso, serão de sua exclusiva responsabilidade, bem como os possíveis danos decorrentes de uso indevido, devendo zelar pelo sigilo de seu acesso.

§ 3º As regras de controle de acesso deverão ser baseadas na premissa de mínimo privilégio, para atendimento das demandas de trabalho do usuário.

Art. 7º Será permitida a criação de apenas uma credencial de acesso por usuário(a).

§ 1º A necessidade de criação de mais de uma credencial para o(a) mesmo(a) usuário(a) fica sujeita à análise da Secretaria de Tecnologia da Informação (STI) e averiguação da justificativa.

§ 2º As credenciais de acesso serão sempre associadas a um(a) usuário(a), serviço ou atividade que as identifique de forma individual, ficando vedado o uso de credenciais de acesso genérico.

Art. 8º O pedido de concessão e de revogação de acesso será formalizado perante a Secretaria de Tecnologia da Informação e será realizado pelos responsáveis definidos pelos gestores dos diversos sistemas e serviços.

§ 1º Compete à Secretaria de Tecnologia da Informação estabelecer e operacionalizar regras de concessão, bloqueio e revogação de acesso aos ativos para os(as) usuários(as), levando em conta as políticas, princípios e normas de controle de acesso aplicáveis.

§ 2º Os acessos deverão ser retirados imediatamente após a revogação dos direitos ou o encerramento das atividades, contratos ou acordos, ou ajustados após qualquer mudança de atribuições.

§ 3º As credenciais deverão ser desabilitadas e movidas para uma Unidade Organizacional (UO) específica, sendo vedada a sua exclusão, com vistas à preservação de dados para eventual auditoria.

Art. 9º A criação de nomes de usuário(a) e de contas de e-mail seguirá critério padronizado, incluindo nome e sobrenome dos(as) usuários(as), salvo disposição em norma específica.

Art. 10. Deverá ser estabelecido e mantido atualizado um inventário de todas as credenciais gerenciadas, contendo data de início e término, incluindo:

I - credenciais de usuário(a) e de administrador(a); e

II - contas de serviço.

§ 1º O inventário das credenciais de usuário(a) e de administrador(a) deverá conter, no mínimo, o nome da pessoa, o nome de usuário(a), telefone e a sua unidade de lotação, enquanto o das contas de serviço indicará ao menos a unidade gestora, serviço vinculado, as datas de revisão e o propósito de uso.

§ 2º As credenciais deverão ser revisadas trimestralmente, ou sempre que necessário, pela unidade responsável, para avaliar se as contas ativas permanecem autorizadas.

Art. 11. A Secretaria de Gestão de Pessoas deverá comunicar, mensalmente, à Secretaria de Tecnologia da Informação, as ocorrências de desligamentos permanentes de servidores(as) em exercício neste Regional (aposentadoria, falecimento, exoneração, etc), magistrados(as), requisitados(as) e estagiários(as), bem como o afastamento em caso de licença por interesse particular.

Parágrafo único. No caso de terceirizados(as), esta comunicação caberá aos(às) gestores(as)/fiscais de seus contratos e/ou à unidade tomadora do serviço.

Art. 12. A Secretaria de Tecnologia da Informação deverá manter inventário dos sistemas de autenticação utilizados pelo Tribunal, abrangendo os internos e aqueles hospedados em provedores remotos.

Seção II

Do Acesso às Redes, Sistemas Internos e Serviços de Rede

Art. 13. A gestão de credenciais de usuários(as) e o controle de acesso se darão de forma centralizada, por meio de serviço de diretório, restrito e controlado pela Secretaria de Tecnologia da Informação.

Parágrafo único. Os direitos de acesso lógico dos usuários(as) à rede corporativa devem ser definidos por meio de credencial e perfil de acesso, de acordo com a sua alocação e função.

Art. 14. É de responsabilidade da chefia imediata da unidade de lotação do(a) usuário(a) solicitar a atribuição/revogação de direitos de acesso aos recursos computacionais do Tribunal, informando os sistemas, serviços, compartilhamentos a serem acessados/revogados e o perfil de acesso que o(a) usuário(a) deverá possuir.

§ 1º A solicitação de acesso/revogação a Juízes Eleitorais ou Desembargadores Eleitorais é de responsabilidade da chefia de cartório e do chefe de gabinete, conforme o caso.

§ 2º A solicitação de acesso/revogação a terceirizados(as), é de responsabilidade do(a) gestor(a) do contrato e/ou da unidade tomadora do serviço.

Art. 15. As autorizações, concessões e revogações devem estar documentadas, para fins de auditoria e levantamento periódico, visando à detecção de usuário(a) com acesso indevido.

Art. 16. A Secretaria de Tecnologia da Informação fará o bloqueio das credenciais de acesso do(a) usuário(a) que não realizar acesso por mais de 60 (sessenta) dias consecutivos.

§ 1º O bloqueio deverá ser informado para o(a) titular da unidade do(a) usuário(a) e, quando possível, para o(a) próprio(a) usuário(a).

§ 2º O desbloqueio de credencial será realizado pela Secretaria de Tecnologia da Informação, mediante solicitação do(a) titular da unidade vinculada ao(à) usuário(a) ou da Secretaria de Gestão de Pessoas.

Art. 17. As atividades de gerenciamento de identidades, acesso e autenticação devem ser registradas e arquivadas.

Parágrafo único. Deverão ser emitidos relatórios, sempre que a Administração entender necessário, para detectar inconsistências nas atividades indicadas no *caput*, atentando-se às recomendações desta portaria, buscando a identificação:

- a) de usuários(as) fora dos padrões de acesso estabelecidos;
- b) de solicitações de acesso sem definição de função ou com cadastro incompleto.

Seção III

Do Acesso Privilegiado e Contas de Serviço

Art. 18. O acesso privilegiado aos sistemas e ativos de informação somente será concedido aos(às) usuários(as) que tenham como atribuição funcional o dever de administrá-los.

§ 1º As credenciais de acesso privilegiado são exclusivas para esse fim e diferem-se daquelas destinadas à realização de atividades normais de negócio pelo(a) usuário(a).

§ 2º Será concedido apenas uma credencial de acesso privilegiado por usuário(a) responsável pela administração de serviços e atividades administrativas, não sendo permitido o uso de credenciais genéricas para desempenho das funções previstas no *caput* deste artigo.

§ 3º Os dados relativos a autorização, concessão e revogação de acesso privilegiado devem ser preservados em sistema próprio para eventual auditoria e levantamento periódico, visando a identificação de usuários(as) com acesso indevido.

§ 4º A solicitação de acesso privilegiado para qualquer unidade que não seja gestora do ativo deverá ser apresentada via processo eletrônico ao Comitê Gestor de Segurança da Informação para análise e autorização.

Art. 19. As contas de serviço são destinadas a um computador ou serviço específico, e serão utilizadas para ações e atividades desenvolvidas para gerenciamento de ativos de TIC, não podendo ser vinculadas diretamente a usuários(as).

§ 1º A criação/revogação de contas de serviço é realizada pela Secretaria de Tecnologia da Informação, unidade responsável pelo gerenciamento e automação dos serviços desempenhados pela TI.

§ 2º As contas de serviço seguem o padrão de segurança definido pela Secretaria de Tecnologia da Informação e serão criadas com informações exclusivas, distintas das credenciais de acesso concedidas a usuários(as) e administradores(as), contendo dados que identifiquem o serviço/atividade vinculada, data de criação, revogação, bloqueio e, sendo possível, o(a) responsável pela manutenção da conta.

§ 3º O acesso das contas de serviço deve possuir privilégios limitados aos ativos e atividades vinculadas, garantindo comunicação, segurança e acesso restrito ao serviço desempenhado.

§ 4º A Secretaria de Tecnologia da Informação realizará o mapeamento e o inventário das contas de serviço utilizadas no ambiente para viabilizar eventual auditoria.

Art. 20. A credencial de acesso privilegiado é de uso pessoal e intransferível, qualificando o(a) usuário(a),

inequívocamente, como responsável por quaisquer acessos e ações realizados com a sua credencial, bem como pelos possíveis danos decorrentes de uso indevido.

Art. 21. Não é permitido o uso de contas de acesso privilegiado para navegação na internet, intranet ou outros serviços e acessos que não sejam, exclusivamente, o de administração/configuração dos ativos.

Art. 22. As competências dos(as) usuários(as) com acesso privilegiado e as funcionalidades das contas de serviço aos sistemas e ativos de informação deverão ser avaliadas em intervalo não superior a três meses, para alinhamento às atividades e observação das regras de segregação de funções.

Art. 23. O acesso privilegiado aos sistemas e ativos de informação deve ser concedido, quando possível, mediante procedimentos de troca periódica de senha e auditoria dos acessos, criados pelo(a) gestor(a) do ativo.

§ 1º Após a saída ou mudança de lotação de usuário(a) com privilégios de administrador(a), suas credenciais devem ser atualizadas.

§ 2º As senhas instituídas deverão ser alteradas, no mínimo, a cada três meses, utilizando padrão de segurança definido pela Secretaria de Tecnologia da Informação.

Art. 24. A credencial administrativa deverá ser desabilitada e movida para Unidade Organizacional (UO) específica, sempre que ocorrer, por qualquer motivo, a revogação do uso de acesso privilegiado e do uso das contas de serviço, sendo vedada a sua exclusão, com vistas à preservação de dados para eventual auditoria.

Art. 25. A Secretaria de Tecnologia da Informação fará o bloqueio das credenciais de acesso privilegiado que não realizarem acesso por mais de 45 (quarenta e cinco) dias.

Parágrafo Único. As contas de serviço deverão ser bloqueadas, imediatamente, quando não estiverem sendo utilizadas para gerenciamento ou controle de ativos de TIC.

Art. 26. As atividades de gerenciamento de identidades, acesso e autenticação com privilégios de administração devem ser registradas e arquivadas.

Parágrafo único. Deverão ser emitidos relatórios para identificar inconsistências nas atividades descritas no *caput* deste artigo, observando-se as recomendações contidas nesta Seção, para as seguintes identificações:

- a) usuários(as) fora dos padrões de acesso estabelecidos;
- b) solicitações de acesso sem definição de função ou com cadastro incompleto.

Seção IV Da Política de Senhas

Art. 27. Os sistemas ou serviços de informação, considerados passíveis de controle de acesso, devem ter seu acesso restrito e controlado através do uso de senhas, *token* ou mecanismo de autenticação similar.

§ 1º O acesso remoto à rede e o acesso a aplicações expostas externamente se darão por autenticação multifatorial (MFA).

§ 2º A Secretaria de Tecnologia da Informação poderá implantar a autenticação de multifatores para determinados tipos de acesso, em função de sua criticidade.

Art. 28. A senha de acesso do(a) usuário(a), *tokens* e outros fatores de autenticação devem ser de uso pessoal e intransferível.

Art. 29. As senhas devem ser secretas e definidas conforme as seguintes recomendações:

I - utilizar números, letras, alternando-as entre maiúsculas, minúsculas e caracteres especiais com, no mínimo, 12 (doze) caracteres para contas com ou sem autenticação de multifatores;

II - não utilizar frases ou palavras que possam ser facilmente adivinhadas por terceiros, baseadas nas

informações relativas ao próprio usuário, tais como nome de parentes, datas de aniversário e números de telefone;

III - não utilizar senhas formadas por sequência de caracteres triviais;

IV - modificar a senha temporária no primeiro logon;

V - não expor a senha em local visível para terceiros, como anotações em papéis, sob pena de responsabilização pelos acessos indevidos.

VI - não utilizar as mesmas credenciais (nome de usuário e senha) para fins pessoais ou profissionais fora do ambiente da Justiça Eleitoral.

Parágrafo único. Sempre que houver indicação de possível comprometimento da senha, o(a) usuário(a) deve realizar sua alteração, bem como comunicar a ocorrência ou a suspeita de comprometimento à Central de Serviços da Secretaria de Tecnologia da Informação.

Art. 30. O sistema de gerenciamento de senha deverá:

I - permitir que os(as) usuários(as) modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;

II - forçar a mudança de senha em intervalos regulares de, no máximo, 6 (seis) meses, conforme necessidade;

III - para o acesso privilegiado, forçar a mudança de senha a intervalos regulares de, no máximo 3 (três) meses, conforme necessidade;

III - manter um registro das senhas anteriores utilizadas e bloquear a reutilização;

IV - empregar criptografia no canal de comunicação utilizado para o tráfego de credenciais de acesso;

V - criptografar ou embaralhar as credenciais de autenticação armazenadas;

VI - não mostrar as senhas na tela quando forem digitadas;

VII - garantir a modificação das senhas temporárias no primeiro acesso ao sistema ou serviço de informação;

VIII - manter, para fins de auditoria, registro dos acessos, das operações e dos respectivos tempos de uso;

IX - desabilitar as contas que não possam ser associadas a um(uma) usuário(a) ou processo de negócio;

X - monitorar tentativas de acesso a contas desativadas.

Art. 31. A senha temporária, criada para primeiro acesso ou sempre que o(a) usuário(a) esquecer a sua senha, deverá ser emitida através de procedimento instruído pela unidade técnica da Secretaria de Tecnologia da Informação, exigindo-se do(a) usuário(a) o fornecimento dos dados pessoais para confirmação de identidade.

Parágrafo único. Fica vedada a emissão de senha para ciência de terceiros, ainda que chefes imediatos ou superiores do(a) usuário(a), bem como o seu envio através de texto não criptografado ou correio eletrônico de terceiro.

Seção V

Dos Procedimentos Seguros de Entrada no Sistema

Art. 32. O procedimento adequado de entrada no sistema (*login*) deve atender às seguintes regras:

I - não fornecer mensagens de ajuda ou informações do sistema, durante o procedimento de entrada, que possam auxiliar usuário(a) não autorizado(a);

II - validar informações de entrada no sistema somente após todos os dados estarem completamente

preenchidos;

III - em caso de erro, não indicar qual parte do dado de entrada está correta ou incorreta;

IV - bloquear o acesso do(a) usuário(a) ao sistema após, no máximo, 5 (cinco) tentativas de entrada no sistema;

V - registrar tentativas de acesso ao sistema, sem sucesso e bem-sucedidas;

VI - por ocasião da entrada no sistema, mostrar as seguintes informações:

a) data e hora da última entrada no sistema ou equipamento, com sucesso; e

b) detalhes de qualquer tentativa sem sucesso de entrada no sistema;

VII - encerrar sessões inativas, após um período definido de inatividade, destacando-se que as estações de trabalho terão suas sessões bloqueadas após 10 minutos de inatividade;

VIII - em caso de uso externo, o tempo de conexão deverá ser restringido para reduzir oportunidade de acesso não autorizado.

CAPÍTULO V DO CONTROLE DE ACESSO FÍSICO

Seção I Do Perímetro de Segurança

Art. 33. Define-se como perímetro de segurança física para proteção das instalações de processamento e armazenamento da informação, os *datacenters* e demais áreas de TI que contenham informações críticas ou sensíveis.

Art. 34. As instalações dos *datacenters* devem atender às seguintes diretrizes:

I - paredes fisicamente sólidas, sem brechas nem pontos por onde possa ocorrer uma invasão, portas protegidas por mecanismos de controle contra acesso não autorizado;

II - videomonitoramento de sua área interna e de seu perímetro;

III - controle de acesso físico às áreas e instalações, utilizando-se dos mecanismos necessários para o controle e registro de data e hora de todas as entradas e saídas, sejam de servidores(as), visitantes ou prestadores(as) de serviço, permitindo-lhes o acesso, desde que previamente autorizados(as);

IV- mecanismos de controle de acesso às áreas críticas, conforme definido pela Secretaria de Tecnologia da Informação;

V - instalações de processamento e armazenamento das informações que sejam projetadas para minimizar os riscos de ameaças físicas potenciais;

VI - edifícios que sejam dotados de proteção contra raios e que, em todas as linhas de entrada de força e de comunicações, tenham filtros de proteção contra raios;

VII - alimentações de energia elétrica e telecomunicações, com rotas físicas diferentes;

VIII - iluminação e comunicação de emergência;

IX - sistema de controle de temperatura e umidade com recurso de emissão de alertas.

Art. 35. As diretrizes para proteção das demais áreas que contenham informações críticas ou sensíveis que não estejam armazenadas nos *datacenters* devem ser estabelecidas pelo Comitê Gestor de Segurança da Informação, observadas as legislações vigentes.

Seção II

Dos Equipamentos de Processamento e Armazenamento

Art. 36. Para evitar perdas, danos, furtos ou comprometimento de ativos e interrupção das operações da organização, o Tribunal deverá observar as seguintes diretrizes:

- I - adotar controles para minimizar o risco de ameaças físicas potenciais e ambientais;
- II - verificar se os suprimentos de energia elétrica, telecomunicações e sistema de ar-condicionado estão em conformidade com as especificações do fabricante do equipamento e com os requisitos legais da localidade, assegurando que os dutos dos suprimentos de água, de gás, de esgoto e de calefação/ventilação predial não passem dentro dos *datacenters*;
- III - adotar controles para evitar a retirada de equipamentos do Tribunal sem prévia autorização da unidade competente, conforme regulamentação específica;
- IV - utilizar, sempre que possível, *racks* que disponham de fechaduras com chave ou mecanismo semelhante, garantindo que apenas a(s) equipe(s) responsáveis pelos ativos instalados nos *racks* possam acessá-los fisicamente.

Seção III

Da Segurança do Cabeamento

Art. 37. O cabeamento de energia elétrica e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos, conforme as seguintes diretrizes:

- I - as linhas de energia elétrica e de telecomunicações que entram nas instalações de processamento da informação devem ser subterrâneas ou suspensas, sempre que possível, e devem atender aos requisitos mínimos de proteção; e
- II - os cabos de energia elétrica devem ser segregados dos cabos de comunicação, para evitar interferências.

Seção IV

Da Manutenção dos Equipamentos

Art. 38. A manutenção dos equipamentos de processamento de informações deve seguir as seguintes diretrizes:

- I - ser realizada somente por pessoal de manutenção identificado e autorizado;
- II - manter registro de todas as falhas, constatadas ou suspeitas, e de todas as operações de manutenção preventiva e corretiva realizadas;
- III - eliminar as informações sensíveis do equipamento, quando possível, ou tratar de forma alternativa os riscos de sua exposição;
- IV - inspecionar o equipamento, após a manutenção, para garantir que não foi alterado indevidamente e que está em perfeito funcionamento.

Seção V

Da Reutilização ou Descarte Seguro dos Equipamentos ou dos Equipamentos em Prova de Conceito

Art. 39. Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização ou descarte, para assegurar que dados sensíveis e *softwares* licenciados tenham sido removidos ou sobregravados com segurança.

§ 1º As mídias que contenham informações com acesso restrito de propriedade intelectual devem ser apagadas fisicamente.

§ 2º As informações a que se refere o parágrafo anterior devem ser destruídas, apagadas ou sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis.

CAPÍTULO VI DISPOSIÇÕES FINAIS

Art. 40. Os casos omissos serão resolvidos pelo Diretor-Geral, ouvindo-se, previamente, o Comitê Gestor de Segurança da Informação (CGSI) do TRE-GO.

Art. 41. Esta norma complementar deve ser revisada a cada 24 (vinte e quatro) meses, ou a qualquer tempo, conforme necessidade, e encaminhada para apreciação do Comitê Gestor de Segurança da Informação.

Art. 42. Esta Portaria entrará em vigor na data de sua publicação.

LEONARDO SAPIÊNCIA SANTOS
Diretor-Geral



Documento assinado eletronicamente por **LEONARDO SAPIÊNCIA SANTOS, DIRETOR-GERAL**, em 16/07/2025, às 14:30, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei4.tre-go.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1157345** e o código CRC **690D9D42**.

